International Journal of Computer Science Engineering
and Information Technology Research (IJCSEITR)
ISSN(P): 2249-6831; ISSN(E): 2249-7943
Vol. 4, Issue 3, Jun 2014, 103-112
© TJPRC Pvt. Ltd.

FINE GRAIN LEVEL TRUST ENHANCEMENT BETWEEN CU AND CSP IN REPLICATION JOBS

SANDEEP SINGH KANG[1] & HARDEEP KAUR[2]

[1]HOD, Department of Computer Science Engineering, Chandigarh Group of Colleges, College of Engineering, Landran, Mohali, Punjab, India

[2]M.Tech Student, Chandigarh Group of Colleges, College of Engineering, Mohali, Punjab, India

ABSTRACT

In this research work we have developed on systematic approach to investigate the concepts related to usage of Third Party Auditor, in cloud computing we have done a tabular analysis of work done by authors in this area with observes in on their outcomes, results and their limitations of work, and based on these findings we have suggest few pointers towards future scope in this area with the observed on facts and figures of the trust levels, degrees between cloud users, cloud service providers and Third Party service providers who help in monitoring and auditing.

KEYWORDS: Trust, Fine Grain Level Trust, Third Party Auditor, Cloud User, Cloud Service Provider

INTRODUCTION

Cloud Computing is very well-known today in IT industry. But in real the Cloud Computing is based on the uses of internet and computer applications. As in cloud computing there are different levels of security issues are. security consideration relates to the various cloud computing service delivery models. The three main cloud service delivery models are: Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) and Software-as-a-Service ss (SaaS).

- **Infrastructure as a Service (IaaS)**

Infrastructure as a Service is a single tenant cloud layer. With contracted clients at a pay-per-use fee the Cloud computing vendor's resources are shared. This help in reducing the effort needed to invest in computing hardware such as networking devices, processing power and servers. In comparison to internal data centre or with collocation services, computing resources can be added or released more cost-effectively and quickly[2]. In internal data centers and collocation services various financial and functional flexibility degrees are not found. IaaS and other associated services have focused own startups. Other businesses gave priority to core competencies without worrying about management of infrastructure and provisioning. IaaS completely focused on the hardware underneath and granted the users to consume infrastructure as a service without much worrying about the underlying complexities. IaaS only provides basic security (perimeter firewall, load balancing, etc.) but the cloud compel value proposition in terms of cost and applications moving into the cloud will need higher levels of security provided at the host.

- **Platform as a Service (PaaS)**

Platform-as-a-Service (PaaS) is a set of software and development tools hosted on the provider's servers. Above IaaS PaaS is the only one layer on the stack and demolishes everything up to OS, middleware, etc. It gives integrated type of privacy to the developer to build their applications without having any clue about what is going on underneath the service. It offers developers a service that provides a complete software development life cycle management, from planning to design to building applications to deployment to testing to maintenance. Everything else is abstracted away from the “view” of the developers. PaaS cloud layer works similarly as IaaS but it gives an additional level of ‘rented’ functionality. PaaS services using clients can transfer more costs from capital investment to operational expenses but they should consider additional constraints and other degrees of lock-in mannered by the additional functionality layers [11]. The use of virtual machines act as a catalyst in the PaaS layer in Cloud computing. Virtual machines must be protected against malicious attacks such as cloud malware. Therefore applications integrity is maintained and well forced accuracy is checked authentically during the transfer of data across the entire networking channels is fundamental. 1.3 Software as a Service

Software-as-a-Service is a software distribution model in which applications are seen by a vendor or service provider and are grossly provided to customers over a network, mainly as the Internet. SaaS is becoming an increasingly accustomed delivery model as underlying technologies that support web services and service-oriented architecture (SOA) [7] nature and new developmental sources become more flourished. SaaS is linked as pay-as-you-go subscription licensing model. During the period the broadband service become more available to the users worldwide. Usually SaaS is implemented to provide business software functionality to the customers at cheap values while allowing the customers to make profits commercially installing the software without complexity. The architecture of SaaS is designed in such a manner to support many concurrent users at once. Using Web Browser over the internet Software applications are accessed. Security officers need to know different methods to secure applications of SaaS. Web Services (WS) security, Extendable Markup Language (XML) encryption, Secure Socket Layer (SSL) these sources and force data protection while transmitting over the internet. Numerous algorithms are used to transfer files and replication in cloud/grid. The Algorithm is used for the file sharing model is Chord Algorithm. By using the dynamic tokens we can transfer the secure data in cloud storage system. File Retrieval and Misleading block checking is done by using Token Computation. Third Party Auditor is also used for the securely send the data between CU and CSP.

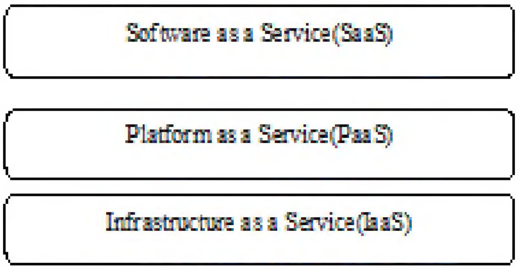

Software as a Service(SaaS)
Platform as a Service(PaaS)
Infrastructure as a Service(IaaS)

Figure 1: Cloud Service Delivery Model

Role of Third Party Auditor: Third party auditor (TPA) is used to audit the outsourced data when needed. The TPA, who has expertise and capabilities that users do not, can time to time check the integrity of all the data that is stored in the cloud on the behalf of the users. In spite of this TPA provide the user benefits of improving their cloud based services. It relieves the user from the storage and computation burden by storing large data files on the remote servers, in the cloud paradigm. So clients must be equipped with certain security that verify the correctness of the remote data without the existence of local copies. In such case where the clients do not have the much time, feasibility or resources to monitor their data, they can delegate the monitoring task to a trusted TPA.

Integrity Verification: The verifier before storing the file at the annals, preprocesses the file and appends some Meta data to the file and stores at the annals. At the time of verification to verify the integrity of the data the verifier uses this Meta data. Protocol of data integrity is to check the integrity of data that is whether the data has been deleted and modified illegally or not. It does not prevent the annals from modifying the data. First of all client will sends the request for checking integrity of data to the TPA for file f(), then TPA will proceeds the request to the Server, then Server will receives the respected file f() from the Server database and produce the Hash code for that file i.e. h(f), and that will be send further to the TPA with file name, TPA will produce the signature i.e. SigGen() from the hash code sent by the Server, TPA will further fetches the old signature from the TPA database i.e. SigPre(),inally TPA will does the equality check between the SigGen() and SigPre() Ack will be sent to the Client depend upon the equality checking. This will be shown in the Figure 2.

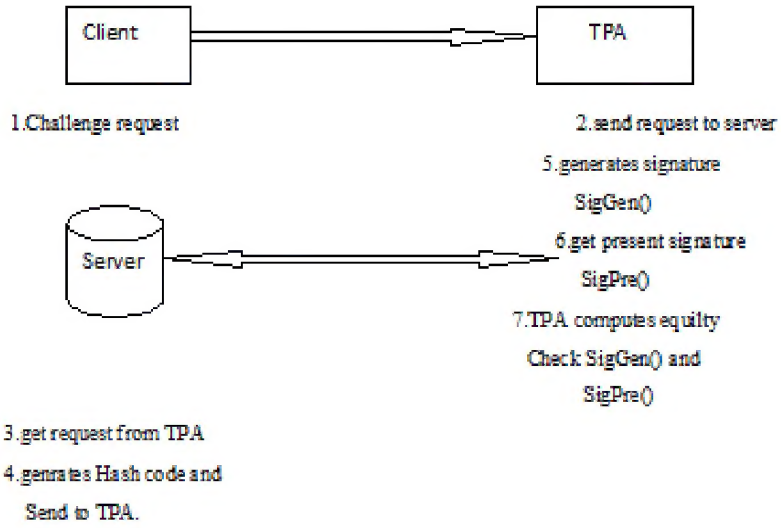


Figure 2

RELATED WORK

We are going to remove the problem of how to enable a privacy-preserving third party auditing protocol at the fine grain level. Korde S.K [2] is work on the batch auditing by using the BLS Algorithm. In the BLS Signature Scheme they used a cryptographic Primitive is called pairing. BLS Signature scheme consists of three phases- Key Generation Phase, compute Signature, Verification phase. It is very lightweight and provable secure provable data possession scheme. This approach caused the minimum overhead and also used the minimize BW. It is not very good in providing protection against the server colluding attacks. Ateniese et al. [4] are the first to consider public auditability in their “provable data possession” (PDP) model for ensuring possession of data files on untrusted storages. For auditing outsourced data and sampling few blocks of the file, they utilize the RSA-based homomorphic linear authenticators. In spite of two proposed schemes, the linear combination of sampled blocks to external auditor is exposed by public auditability scheme. Data information may leak to the external auditor when used directly. For this loop pole Cong Wang (2013) [3] worked on the privacy-preserving public auditing system for data storage security in cloud computing (storage). Homomorphic linear authenticator (HLA) and random masking technique are used by them to guarantee that the TPA will preserve their knowledge about the data content stored on the cloud. TPA jointly handles multiple audit sessions from many users for their outsourced data files. Deswarte et.al. [5] applied RSA-based hash functions to hash the entire file at every challenge. This is clearly prohibitive for the server whenever the file is large.

RESEARCH GAP

After conducting exhaustive systematic literature survey and are possible solicited material associated with topic from various journals conferences material we can say limited work has been done which at fine grain level (file block level) auditing, monitoring with authentication is done using Third Party service providers in replication on demand jobs scheduling in cloud providers. Hence, the existing work can move in this direction and improve this system.

PROPOSED WORK

Cloud Resource virtualized data centre class. It handles VM processing queries (i.e., handling of VMs) instead of processing Cloudlet-related queries. The Cloud User is an object which generates the workload and submit to the Data Centre. It is an object that seeking services from the Cloud Service Provider.

As per the block no.3 after the data centre broker we initialize the TPA. TPA process the data/audit the data so that it can reduce the online burden of the users. TPA is the third party or we can say that the middle party that do not give them any information about the CU to CSP and the vice versa i.e. it secured/hides the data from each other. Workload specification is the class of a host supporting dynamic workloads and performance degradation. Data files like ASCII text, Zip files, gzip are our workload that is send by the user to cloud. Workload model is also read the resources from the file and creating a list of job. Links, policy, Peak Load, Off Peak Load, Holiday Load are used as the grid resources. GIS is the Grid Information Service.

We set the regional GIS entity for the Grid Resources to communicate it. Any upcoming new Grid Resource should register to region GIS. After registering the Grid Resources to GIS we use the VM Allocation Policy so that we can process the VM's. Work replication catalog tells about the list of resources ID's that store in the given logical file name (lfn). After that we use the Global RC that means a RC that is registered to other region GIS entities. TPA Log Harmonizer is to hold the log file corruption and after that the logger sends the error correction information in to the log harmonizer.

Next, Individuals records are hashed together to create a chain structure, able to quickly detect possible errors or missing records. In the FIFO scheduling there is no buffer management so packets can never be dropped and the queue can grow as long as system memory is available. Packets are enqueued by this scheduler. Number of blocks is calculated/ evaluated by using the formula is given below:-

No. of Blocks = File Size*7.5

MKT is used to divide the file into blocks. It allows efficient and secure verification of the contents of large data structure. The values of data blocks are authenticated by using the MKT. It is made as a binary tree. Integration of data should be checked after the verification of CS, CSP credentials. First of all the encrypted data is decrypted here and after that the integrity of data is checked by the TPA. First of all the file sends to CSP by the CU. After that the file retrieves by the TPA and verifies its signature if it fails then it sends the false message to CSP. TPA also does the verification on the Gen Proof that is generated by the CSP for the challenge that is send to CSP by the TPA. Similarly it verifies it through the Verify Proof if verification fails file is rejected and if not the file is accepted.

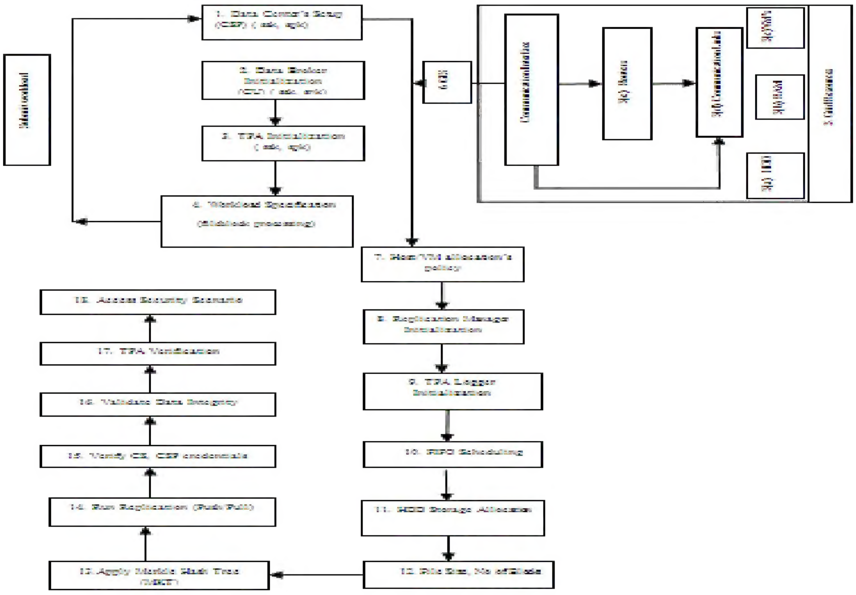

1. Data Owner's Setup (CSP) (ssk, spk)
2. Data Broker Initialization (CU) (ssk, spk)
3. TPA Initialization (ssk, spk)
4. Workload Specification (Subblock processing)
7. Host/VM allocation's policy
8. Replication Manager Initialization
9. TPA Logger Initialization
10. FIFO Scheduling
11. HDD Storage Allocation
12. File Size, No of Block
13. Apply Merkle Hash Tree (MHT)
14. Run Replication (Push/Pull)
15. Verify CU, CSP credentials
16. Validate Data Integrity
17. TPA Verification
18. Access Security Scenario

Figure 3: Workflow Chart

RESULTS AND CONCLUSIONS

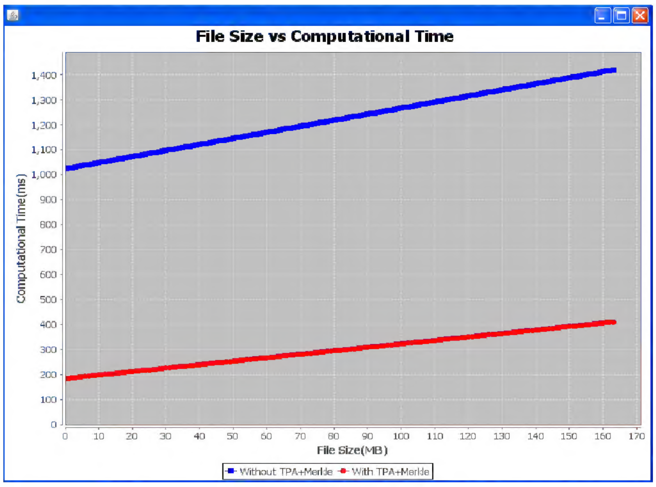
We have make the trust enhancement between the CU and CSP at the fine grain level by using the method/algorithm TPA + Merkle. Here we first make the comparison table on the behalf of results.

Table 1: Performance of Our Scheme under Different File Size and No of Replication Jobs

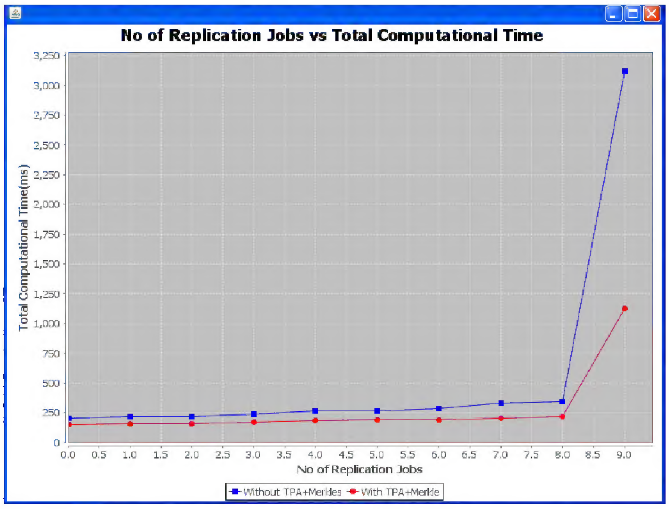
	Our Scheme	Previous
File Size(MB)	1-165	1-165
Min comp. time(ms)	183	1024
Max comp. time(ms)	409	1419

	Our Scheme	Previous
No of replication job	10	10
Min total comp. time(ms)	157	203
Max total comp. time(ms)	1125	3125

The graphs are shown below for file size v/s computational time that shows graphically is our scheme takes lesser time than that of previous one.:



The next graph shown below is for no of replication jobs versus total computational time:-



CVSS Scoring without Hardening

The man in the middle attack under study was simulated and CVSS [18] score before hardening was calculated in order to objectively measure vulnerability of the system.

Table 2

Base Metric	Metric Value	
Access Vector	Network (N)	1
Access Complexity	Low (L)	71
Authentication	Multiple (M)	45
Confidentiality Impact	Complete (C)	660
Integrity Impact	Complete (C)	660
Availability Impact	Partial (P)	275

Base score = [(.6*impact)+.4(exploitability)- 1.5]*f(impact)

Impact = 10.41*[1-(1-confimpact)*(1-integimpact)*(1-availimpact)]

Exploitability = 20*Access Vector*Access Complexity*Authentication

From Equation 2

Impact = 10.41[1-(1-.660)*(1-.660)*(1-.275)]

= 9.53

From Equation 3

Exploitability = 20*1*.71*.45 = 6.39

From Equation 1

Base Score = [.6(9.53)+.4(6.39)-1.5]*1.176

= 8

So CVSS before hardening was 8 which is fairly high on 0-10 point CVSS scale [0 indicating completely secure network and 10 indicating completely vulnerable network].

CVSS Score after Hardening

Table 3

Base Metric	Metric Value	
Access Vector	Network (N)	1
Access Complexity	Low (L)	.71
Authentication	Multiple (M)	.45
Confidentiality Impact	Partial (P)	.275
Integrity Impact	Partial (P)	.275
Availability Impact	None	0

Impact = 4.9 (calculates from equation 2)

Exploitability = 6.39 (calculates from equation 3)

Base score = 4.7 (calculates from equation

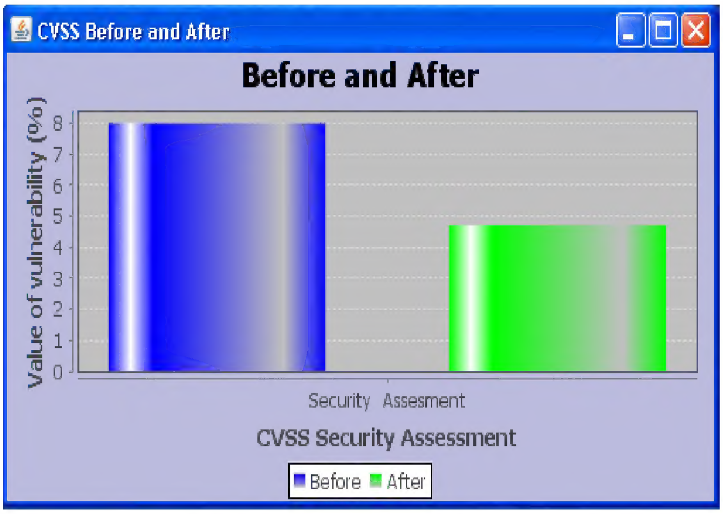


Figure 4: CVSS before and after Hardening

Figure 3 and 4 provide and insight into comparison of security and vulnerability of the network before and after hardening

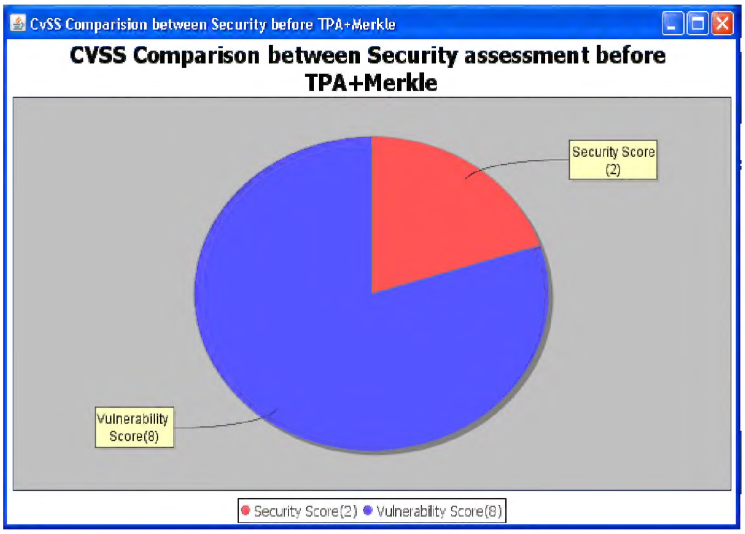


Figure 5: CVSS Comparison before Hardening

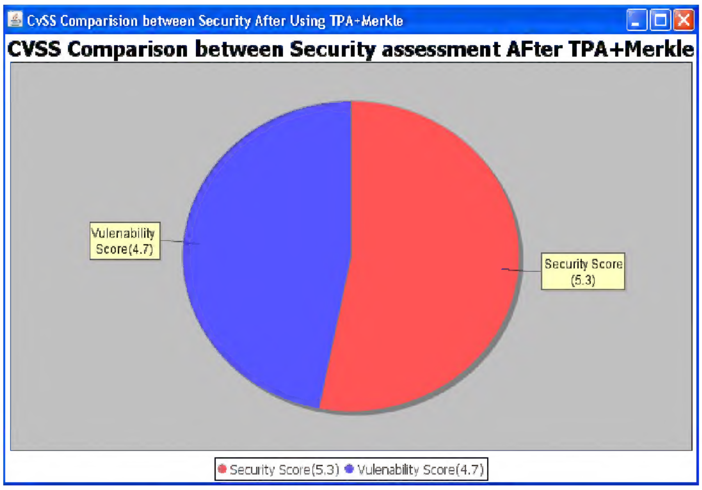


Figure 6: CVSS Comparison after Hardening

CONCLUSIONS

In this research work we have developed a new for securing the data replication services in cloud based platform , and the approach was to build a fine grain level security with monitoring when the data is transferred from one source to destination as per the replication catalog of the cloud service provider, for this we found the use of Merkle algorithm with security auditing at file block level not only enchases the security but reduces probability the possibility of any attack like man in the middle , which is apparent from the security assessment score in the pie charts. All these assessment chart values shows that the workflow the data replication service is hardened better and more.

FUTURE SCOPE

In days come automated software components or agents will interact with each other and there will be a need for machine to machine trust algorithms as many applications will run 24 hours without human interface, represented by robotic interfaces. Hence, there will be need to build machine to machine trust based algorithms, the future direction may work in direction to secure the cloud based applications.

REFRENCES

1. Vinaya. V, Sumathi. P (2013), Implementation of Effective Third Party Auditing for Data Security in Cloud.
2. Jachak K.B.*, Korde S.K., Ghorpade P.P, Garge G. j. (2012), Homomorphic Authentication With Randim Masking Technique Ensuring Privacy & Security In Cloud Computing.
3. Cong Wang, Sherman S.M. Chow, Qian Wang, Kui Ren and Wenjing Lou (2013), Privacy-Preserving Public Auditing for Secure Cloud Storage.
4. G. Ateniese, R. Burns, R. Curtmola, J. Herring, L. Kissner, Z. Peterson, and D. Song (2007), Provable Data Possession at Untrusted Stores.
5. Y. Deswarte, J.-J. Quisquater, and A. Saidane (2003), Remote integrity checking.
6. D. L. G. Filho and P. S. L. M. Baretto (2006), Demonstrating data possession and uncheatable data transfer.
7. Kuyoro S. O., Ibikunle F., Awodele O. (2011), Cloud Computing Security Issues and Challenges.

8. Francisco Moyano, Carmen Fernandez-Gago and Javier Lopez(2013) A Framework for Enabling Trust Requirements in Social Cloud Applications.

9. Neil Robinson, Lorenzo Valeri, Jonathan Cave & Tony Starkey(RAND Europe) Hans Graux (time.lex) Sadie Creese & Paul Hopkins (University of Warwick) (2010) The Cloud: Understanding the Security, Privacy and Trust Challenges.

10. Ashish Bhagat Ravi Kant Sahu (2013) Using Third Party Auditor for Cloud Data Security: A Review.

11. Armbrust,M., Fox, A.,Griffith, R., Joseph, A.D.,Katz, R.H., Konwinski, A., Lee, G., Patterson, D.A., Rabkin, A., Stoica, I., Zaharia, M.(2010) A view of cloud computing. Commun.

AUTHOR'S DETAILS

Dr. Sandeep Singh Kang Working at CGCCOE Landran as HOD (CSE) Since Nov, 2007. 2013. He did his B. Tech from Punjab Technical University and M. Tech from Punjabi University Patiala. Recently he has Completed his Ph. D in Computer Science & Engineering in the area of Wireless Networks. He has total of 10 years of Experience. He has Published 52 Research Papers in International/National Journals and Conferences and attended 12 workshops and FDP's for enhancement of his skills. He has Published a BOOK Title: "**Integrated Approach to Network Security".** Besides this, he has guided around 20 Students for PG Research Work and guiding 02 students for doctorate. His area of specialization is Security of Wireless Networks. He is the Life Member of Computer Society of India and Member Board of Studies (Computer Science), Punjab Technical University, Jalandhar.

Hardeep Kaur received the B. Tech degrees in Computer Science & Engineering from Shaheed Udham Singh College of Engg & Technology (Tangori) Punjab in 2011 and Now Pursuing M.Tech (2011-2013) in Computer Science & Engg in Chandigarh Group of colleges College of Engg & Technology (Landran)